Practical decoy state method in quantum key distribution with heralded single photon source

Qin Wang[1],* Xiang-Bin Wang[2], and Guang-Can Guo[1]

[1]*Key Laboratory of Quantum Information, Department of Physics,*
University of Science and Technology of China,
Hefei 230026, People's Republic of China and
[2]*Department of Physics, Tsinghua University, Beijing 100084, China*

Abstract

We propose a practical decoy state method with heralded single photon source for quantum key distribution (QKD). In the protocol, 3 intensities are used and one can estimate the fraction of single-photon counts. The final key rate over transmission distance is simulated under various parameter sets. Due to the lower dark count than that of a coherent state, it is shown that a 3-intensity decoy-state QKD with a heralded source can work for a longer distance than that of a coherent state.

PACS number(s): 03.67.Dd, 42.65.Yj, 03.67.Hk

*Electronic address: wq0305@ustc.edu

I. INTRODUCTION

As is well known that, a two-mode light source, such as the state from a parametric down conversion (PDC) or a two-mode squeezed state takes a very important role in quantum information processing (QIP)[1]. Since the two modes always have same number of photons, one mode can be used to indicate the state of the other, therefore it is also called heralded single photon source (HSPS). Moreover, recent years, due to its wide applications in many fields, such as in quantum information and quantum radiometry *etc.,* the technology on how to efficiently obtain HSPS has been developed to a high level [2, 3, 4, 5, 6, 7, 8, 9, 10].

In the past few years, quantum key distribution has attracted extensive attentions for its unconditional security compared with conversional cryptography [11, 12, 13, 14, 15, 16]. However, there still exist some limitations in practice, such as imperfect single source, large loss channel and inefficient detectors *etc.*. Under such limitations, one serious threaten to the security is the so called photon number splitting attack[17, 18, 30]. Fortunately, a number of methods and proposals have been presented for secure QKD even with these imperfections. These include the mixed protocol[19], the strong-reference light method[20], and the decoy-state method[21, 22, 23, 24]. And in this paper, what we are interested with is the decoy-state method. Firstly, according to the separate result of ILM-GLLP, we can distill a secure final key even an imperfect source is used, provided that we know the lower bound of fraction of single photon-counts[21]. The non-trivial problem on how to verify a tight lower bound was not answered then. Later, Hwang[22] proposed the decoy state method to verify such a lower faithfully.

After that, decoy state method has been advanced by several researchers [23, 24, 25, 26, 27]. The main idea there is to randomly change the intensity of each pulses among different values, and then deduce the lower bound of fraction of single-photon counts according to the observed counts of different intensities. In particular, it has been shown that, one can make a very tight estimation, i.e., the estimated lower bound is only a bit larger than the true value therefore a good final key rate can be obtained by only using 3 intensities, $0, \mu, \mu'$[23] or 4 intensities[25].

However, using the coherent states, the dark count will be significant given a distance longer than 100 kilometers. Naturally, one may think about using HSPS to decrease the effect of dark count. In fact, as it has been shown recently, an HSPS can indeed raise the distance for QKD if one knows the channel transmittances of each photon number states exactly[28]. However, knowing these exactly requires using infinite number of intensities. This seems to be an impossible task in practice. Very recently, it is proposed to use photon-number-resolving detectors to do decoy-state QKD with HSPS[29].

In this paper, we will propose a practical decoy state method with HSPS. We only need 3 intensities and normal yes-no single-photon detectors at Bob's side. That is to say, we only assume the technologies that have already adopted in the existing set-ups.

This paper is organized as follows: In Sec. II, starting from the two-mode state, we shall then present the main result of our protocol, i.e., the lower bound of single-photon counts. In Sec. III, we estimate the QKD distance of our method in various settings. This work is concluded in Sec IV.

II. HERALDED SINGLE PHOTON SOURCE

Given a two-mode state of the form

$$|\chi\rangle = \cosh^{-1}\chi \sum_{n=0}^{\infty} e^{in\theta}\tanh^{n}\chi|n,n\rangle. \tag{1}$$

The averaged photon number in one mode is $\sinh^2\chi$ and we shall use this value to indicate the pulse intensity, i.e., when we say that we use intensities of $0, \mu, \mu'$ for the two mode state as described by Eq.(1), we mean that $\sinh^2\chi = 0, \mu, \mu'$, respectively.

As indicated in Ref. [30], after triggering out one of a photon pair, the other mode is basically a thermal field of distribution :

$$\rho_x = \frac{1}{P_{post}(x)}\left\{\frac{d_A}{1+x}|0\rangle\langle 0| + \sum_{n=1}^{\infty}\left[1-(1-\eta_A)^n\right]\frac{x^n}{(1+x)^{n+1}}|n\rangle\langle n|\right\}, \tag{2}$$

where x is the mean photon number of one mode (before triggering), η_A, d_A for the detection efficiency and dark count rate of Alice's detector and the post-selection probability is $P_{post}(x) = \frac{d_A}{1+x} + \frac{x\eta_A}{1+x\eta_A}$. The detectors assumed in our protocol here are threshold detectors, i.e., the outcome of each individual measurement is either clicking or not clicking.

In the protocol, we request Alice to randomly change the intensities of her pump light among 3 values, so that the intensity of one mode of the two mode source is randomly changed among $0, \mu, \mu'$ (and $\mu' > \mu$). We define Y_n to be the yield of a n-photon state, i.e., the probability that Bob's detector click whenever Alice sends out state $|n\rangle$. We also denote the yield state $\rho_\mu, \rho_{\mu'}$ by $Y_\mu, Y_{\mu'}$. In the protocol, one can immediately know the value of Y_0 by watching the counts of vacuum pulses, and one can also know the value of $Y_\mu, Y_{\mu'}$ by watching the counts caused by pulses of intensity μ, μ' respectively. In particular, suppose there are N_x pulses for state ρ_x and N_{xt} of them are triggered. During the time windows of these N_{xt} pulses, Bob has observed n_x clicks. Then we have $Y_x = n_x/N_{xt}$ according to our definition of yield. We want to deduce the value of Y_1 based on the known parameters Y_0, Y_μ and Y'_μ. Similar to the case of coherent states[23], we can verify the lower bound of Y_1 by the following constraints:

$$\tilde{Y}_\mu = Y_0 \frac{d_A}{1+\mu} + \sum_{i=1}^{\infty} Y_n \left[1-(1-\eta_A)^n\right] \frac{\mu^n}{(1+\mu)^{n+1}}, \tag{3}$$

and

$$\tilde{Y}_{\mu'} = Y_0 \frac{d_A}{1+\mu'} + \sum_{i=1}^{\infty} Y_n \left[1-(1-\eta_A)^n\right] \frac{\mu'^n}{(1+\mu')^{n+1}}, \tag{4}$$

and $\tilde{Y}_x = (N_{xt}/N_x)Y_x$, $x = \mu, \mu'$. These two equations lead to

$$\begin{aligned}
&(1+\mu)\left(\frac{\mu'}{1+\mu'}\right)^2 \tilde{Y}_\mu - (1+\mu')\left(\frac{\mu}{1+\mu}\right)^2 \tilde{Y}_{\mu'} \\
&= Y_0 \frac{d_A}{1+\mu}\left(\frac{\mu'}{1+\mu'}\right)^2 - Y_0 \frac{d_A}{1+\mu'}\left(\frac{\mu}{1+\mu}\right)^2 \\
&+ \eta_A Y_1 \left[\frac{\mu}{1+\mu}\left(\frac{\mu'}{1+\mu'}\right)^2 - \frac{\mu'}{1+\mu'}\left(\frac{\mu}{1+\mu}\right)^2\right] \\
&+ \sum_{n=3}^{\infty} Y_n \left[1-(1-\eta_A)^n\right] \left[\frac{\mu^n \mu'^2}{(1+\mu)^n (1+\mu'^2)} - \frac{\mu'^n \mu^2}{(1+\mu'^n (1+\mu^2)}\right].
\end{aligned} \tag{5}$$

It is easy to see that for any $n \geq 3$, $\frac{\mu^n \mu'^2}{(1+\mu)^n (1+\mu'^2)} - \frac{\mu'^n \mu^2}{(1+\mu'^n (1+\mu^2)} < 0$ given that $\mu' > \mu$. Therefore Eq.(5) leads to the following inequality:

$$\begin{aligned}
Y_1 \geq &\left\{\frac{\mu'}{\mu}(1+\mu)^3 \tilde{Y}_\mu - \frac{\mu}{\mu'}(1+\mu'^3 \tilde{Y}_{\mu'} - Y_0 d_A \left[\frac{\mu'}{\mu}(1+\mu)^2 - \frac{\mu}{\mu'}(1+\mu'^2\right]\right\} \times \\
&[\eta_A(\mu'-\mu)]^{-1}
\end{aligned} \tag{6}$$

This gives rise to the fraction of single-photon counts for the triggered pulses of different intensities by the following formula

$$\Delta_1(x) = \frac{Y_1 \eta_A x}{Y_x P_{post}(x)(1+x)^2} \tag{7}$$

and x can be μ or μ' here. Also, if we have observed the quantum bit-flip rate (QBER) for triggered pulses of intensity x is E_x, we can upper bound the QBER value for those single-photon pulses by

$$e_1 \leq \frac{(1+x)^2 E_x \tilde{Y}_x - (1+x) Y_0 d_A/2}{Y_1 \eta_A x}. \tag{8}$$

Normally, we use the value from $x = \mu$ for a tight estimation of e_1. Given all these, we can use the following formula to calculate the final key-rate of triggered signal pulses:

$$R \geq \frac{Y_{\mu'} P_{post}(\mu')}{2} \left\{ -f\left(E_{\mu'}\right) H_2\left(E_{\mu'}\right) + \Delta_1(\mu') \left[1 - H_2\left(e_1\right)\right] \right\} \tag{9}$$

where the factor $\frac{1}{2}$ comes from the cost of basis miss-match in Bennett-Brassard 1984 (BB84) protocol; $f(E_{\mu'})$ is a factor for the cost of error correction given existing error correction systems in practice. We assume $f = 1.2$ here. $H_2\left(x\right)$ is the binary Shannon information function, given by

$$H_2\left(x\right) = -x \log_2(x) - (1-x)\log_2(1-x).$$

III. NUMERICAL SIMULATION

In an experiment, we only need to observe the values of $Y_0, Y_\mu, Y_{\mu'}$ and $E(\mu), E_{\mu'}$ and then deduce the lower bound of fraction of single-photon counts and upper bound QBER of single-photon pulses by the theoretical results and then one can distill the secure final key.

Here our goal is to theoretically estimate the final key rate of our protocol if we really *did* the experiment. In principle, whatever possible results can be observed in an experiment. In evaluating our the efficiency of our protocol theoretically, we shall only consider the normal case where there is no Eve and we calculate the key rate with respect to distance. In order to make a faithful evaluation, we first need a model to forecast what values for $Y_0, Y_\mu, Y_{\mu'}, Y_\mu$ and $E(\mu), E_{\mu'}$ *would* be observed if we *did* the experiment in the case there is no Eve. After these values are estimated, we can calculate the final key rate by Eq.(9) therefore the efficiency is evaluated theoretically.

Suppose η is the overall transmittance and detection efficiency between Alice and Bob; t_{AB} is the transmittance between Alice and Bob, $t_{AB} = 10^{-\alpha L/10}$; η_B is the transmittance in Bob's side, $\eta = t_{AB}.\eta_B$. Therefore normally, the observed value for $Y_\mu, Y_{\mu'}$ should be around

$$Y_x = \frac{1}{P_{post}(x)} \left\{ \frac{d_A d_B}{1+x} + \sum_{n=1}^{\infty} \frac{[1-(1-\eta_A)^n]x^n}{(1+x)^{n+1}} [d_B + 1 - (1-\eta)^n] \right\} \tag{10}$$

and x can be any of μ, μ', d_B is the dark count rate of Bob's detector. This leads to

$$\tilde{Y}_x = \frac{d_A d_B}{1+x} + \sum_{n=1}^{\infty} \frac{[1-(1-\eta_A)^n]x^n}{(1+x)^{n+1}} [d_B + 1 - (1-\eta)^n] \tag{11}$$

and $\tilde{Y}_x = Y_x \cdot P_{post}(x)$ is directly used in Eq.(6), Eq.(7) for calculating the single-photon counts.

We use the following for the error rate of an *n-photon* state:

$$e_n = \frac{e_0 d_B + e_d[1-(1-\eta)^n]}{d_B + 1 - (1-\eta)^n} \tag{12}$$

where $e_0 = 1/2$, d_B is dark count rate of Bob's detectors, e_d is the probability that the survived photon hits a wrong detector, which is independent of the transmission distance. Below we shall assume e_d to be a constant. Therefore, the observed E_μ value should be around

$$E_x = \frac{e_0 d_B}{Y_x} + \frac{1}{Y_x P_{post}(x)} \sum_{n=1}^{\infty} \frac{e_d x^n [1-(1-\eta_A)^n][1-(1-\eta)^n]}{(1+x)^{n+1}}. \tag{13}$$

In practical implementation of QKD, we often use the non-degenerated down-conversion to produce photon pairs, with one photon at the wavelength convenient for detection acting as heralding signal, and the other falls into the telecommunication windows for optimal propagation along the fiber or in open air acting as heralded signal. To illustrate the calculation, we assume the heralding photon is adapted to be 800nm, and the heralded one to be 1550nm. We shall use these formulas and experimental parameters of GYS as listed in table I to simulate the observed values Y_μ, $Y_{\mu'}$ for Eq.(6,7) and the calculate the final key rate by Eq.(9).

We can now calculate the final key generation rate with the assumed observed values above. For convenience of comparing with the result of coherent states, we use the same parameters as in GYS [31], shown in Table I, and $d_A = 10^{-5}$. Our simulation results are shown in Fig. 1, Fig. 2 and Fig. 3.

Fig. 1 shows with HSPS the key generation rate against transmission distance in the asymptotic decoy state method and in our practical two decoy state method, we use different intensity of weak decoy state ($\mu = 0.01, 0.05, 0.10$) respectively. From the curves in Fig. 1, we

FIG. 1: Table1. Experimental parameters in GYS.

Experiment	λ (nm)	α dB/km)	e_d (%)	Y_0	η_B	f (MHz)
GYS	1550nm	0.21	3.3	1.7×10^{-6}	0.045	2

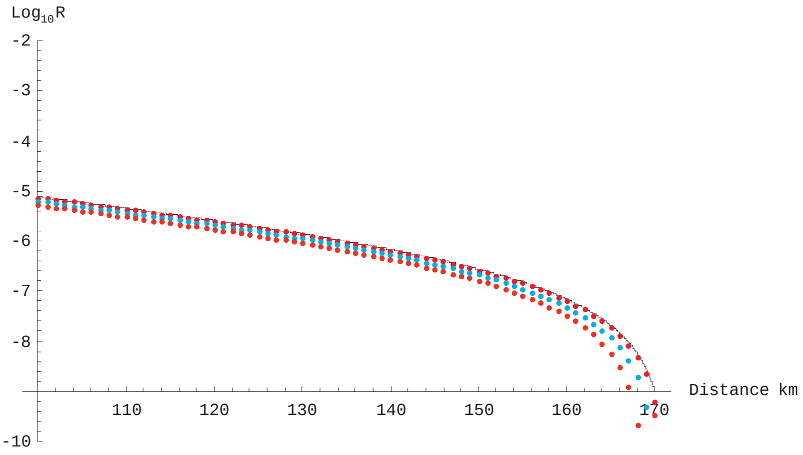

FIG. 2: Fig1. Final key rates vs transmission distance for decoy state method with an HSPS source. The black solid line is the ideal result where the fraction of single-photon counts and QBER of single-photon pulses are known exactly. The dotted lines are the results of our 3-intensity decoy state method with $\mu = 0.01, 0.05, 0.10$, from upper to down. (μ' has the optimal value at each point.)

can see that our 3-intensity decoy state method can asymptotically approach the theoretical limit of ideal case.

Fig. 2 shows different key generation rate comparing HSPS ($\eta_A = 0.8$) with WCS.

Fig. 3 shows the same objects as in Fig. 2 except with $\eta_A = 0.6$.

From these simulations above, we can see that, our proposal can significantly raise the transmission distance compared with that of coherent states even with imperfect triggering detector ($\eta_A = 0.6$). However, it has a lower key generation rate. The reasons are as follows: On one hand, in HSPS the dark count probability is so low by Alice's triggering system, there the transmission distance is raised, on the other hand, an HSPS is basically a thermal field which has a higher multi-photon probability than that in Poissonian distribution with

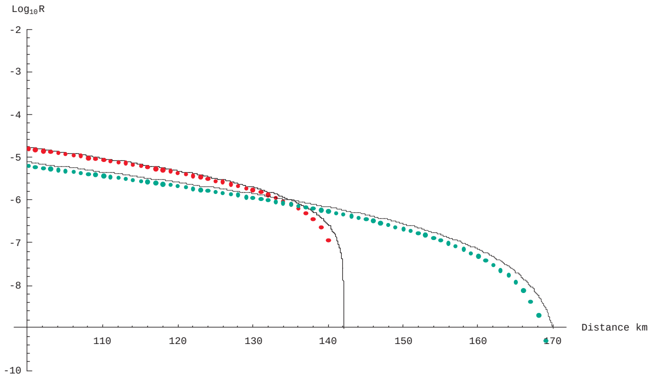

FIG. 3: Fig2. Comparison of final key rate between a 3-intensity decoy-state protocol with an HSPS source and the one with a coherent state source. The solid lines are for the ideal results and the dotted lines are for 3-intensity protocols. The green dotted line represents the result of an HSPS source (with $\eta_A = 0.8$, $\mu = 0.05$), and the red dotted line represents the results of a coherent state source (with $\mu = 0.05$). (μ' has the optimal value at each point.)

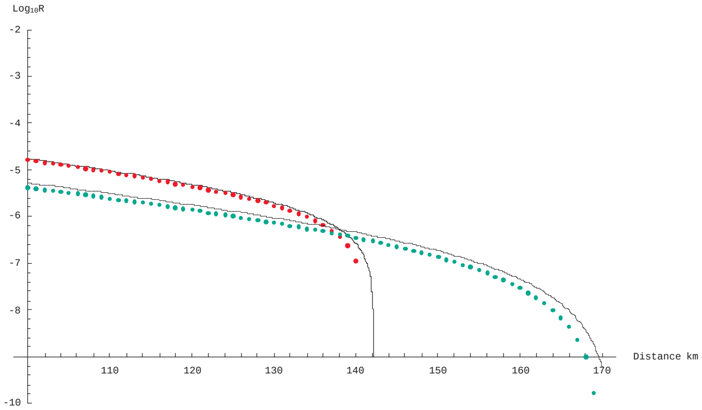

FIG. 4: Fig3. Key rate vs transmission distance. It shows the same objects as in Fig. 2, but here we have set $\eta_A = 0.6$.

the same mean photon number, therefore the key rate is decreased.

IV. CONCLUDING REMARK.

In summary, we have presented a practical decoy state method in quantum key distribution with a heralded single photon source. By using 3 intensities, 0, μ, μ', we can estimate the lower bound of single-photon counts and the upper bound of single-photon QBER rather tightly. Moreover, our simulation results show that, the transmission distance of our 3-intensity decoy-state QKD protocol with HSPS is larger than that of with weak coherence states. Therefore, our 3-intensity decoy state method with HSPS seems to be a promising candidate in practical implementation of quantum key distribution.

Acknowledgement

Qin thanks Tomoyuki Horikiri (Univ. Tokyo) and Prof. Norbert Lütkenhaus (Univ. Waterloo) for useful discussions. This work is supported by National Fundamental Research Program (2001CB309300), Tsinghua Bairen Program, the Innovation Funds from Chinese Academy of Sciences, Program for New Century Excellent Talents in University.

[1] D. N. Klyshko, Photons and Nonlinear Optics, Gordon and Breach Science Publishers, 1988.

[2] S. Fasel *et al.*, New J. Phys., **6**, 163 (2004).

[3] M. A. Albota, E. Dauler, J. of Mod. Opt., **51**, 1417 (2004).

[4] C. Kurtsiefer, M. Oberparlieter, H. Weinfurter, Phys. Rev. A, **64**, 023802 (2001).

[5] S. Castelletto, Degiovanni I. P., V. Schettini, A. Migdall, SPIE Proc., **5551**, 60 (2004).

[6] D. Ljunggren, M. Tengner, quant-ph/0507046.

[7] F. A. Bovino, P. Varisco, A. M. Colla, G. Castagnoli, G. Di Giuseppe, A. V. Sergienko, Opt. Comm., **227**, 343 (2003).

[8] T. B. Pittmann, B. C. Jacobs, J. D. Franson, Opt. Commun., **246**, 545 (2005).

[9] S. Castelletto, I. P. Degiovanni, V. Schettini and A. Migdall, Opt. Exp., **13**, 6709 (2005).

[10] S. Castelletto, I. P. Degiovanni, V. Schettini and A. Migdall, quant-ph/0601067.

[11] C. H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), p. 175.

[12] D. Mayers, J. ACM, **48**, 351 (2001).

[13] P. W. Shor and J. Preskill, Phys. Rev. Lett., **85**, 441 (2000).

[14] A. K. Ekert and B. Huttner, J. Mod. Opt., **41**, 2455 (1994).

[15] D. Deutsch *et al.*, Phys. Rev. Lett., **77**, 2818 (1996).

[16] D. Deutsch *et al.*, Phys. Rev. Lett., **80**, 2022(E) (1998).

[17] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); H. P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996).

[18] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).

[19] V. Scarani, A. Acin, G. Robordy, N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004); C. Branciard, N. Gisin, B. Kraus, V. Scarani, Phys. Rev. A **72**, 032301 (2005).

[20] M. Koashi, Phys. Rev. Lett., **93**, 120501 (2004); K. Tamaki, N. Lükenhaus, M. Loashi, J. Batuwantudawe, quant-ph/0608082.

[21] H. Inamori, N. Lütkenhaus, D. Mayers, quant-ph/0107017; D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[22] W. Y. Hwang, Phys. Rev. Lett., **91**, 057901 (2003).

[23] X. B. Wang, Phys. Rev. Lett., **94**, 230503 (2005).

[24] H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett., **94**, 230504 (2004).

[25] X. B. Wang, Phys. Rev. A, **72**, 012322 (2005).

[26] X. Ma, B. Qi, Y. Zhao, and H. K. Lo, Phys. Rev. A, **72**, 012326 (2005).

[27] J. W. Harrington *et al.*, quant-ph/0503002.

[28] T. Horikiri and T. Kobayashi, Phys. Rev. A, **73**, 032331 (2006).

[29] W. Mauerer and C. SIberhorn, quant-ph/0609195.

[30] N. Lütkenhaus, Phys. Rev. A, **61**, 052304 (2000).

[31] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett., **84**, 3762 (2004).

Caption:

Fig 1. Final key rates vs transmission distance for decoy state method with an HSPS source. The black solid line is the ideal result where the fraction of single-photon counts and QBER of single-photon pulses are known exactly. The dotted lines are the results of our 3-intensity decoy state method with $\mu = 0.01, 0.05, 0.10$, from upper to down. (μ' has the optimal value at each point.)

Fig 2. Comparison of final key rate between a 3-intensity decoy-state protocol with an HSPS source and the one with a coherent state source. The solid lines are for the ideal results and

the dotted lines are for 3-intensity protocols. The green dotted line represents the result of an HSPS source (with $\eta_A = 0.8$, $\mu = 0.05$), and the red dotted line represents the results of a coherent state source (with $\mu = 0.05$). (μ' has the optimal value at each point.)

Fig 3. Shows the same objects as in Fig. 2 but here we have set $\eta_A = 0.6$.